Rechtliche Aspekte von Penetrationstests

Die Prüfdisziplin Penetrationstest existiert seit ungefähr 15 Jahren, etabliert hat sich das Testverfahren jedoch erst in den letzten fünf. Dabei ist festzustellen, dass Penetrationstests zunehmend an Bedeutung gewinnen und Unternehmen vor allem darin dienen, ihre eigene IT-Umgebung gegen Angriffe und Missbrauch abzusichern. Da die Durchführung dieser Tests jedoch rechtlich nicht immer einfach ist, hat dieser Artikel die Absicht, rechtliche Aspekte bei der Umsetzung von Penetrationstests anzusprechen.

Von Sebastian Schreiber

Kaum ein Tag vergeht, an dem die Medien nicht über Hackerangriffe berichten. Ob in der Öffentlichkeit aufgetauchte persönliche Daten von zigtausenden Studenten, immer wieder auftretende Fälle, wie Menschen hinterrücks auf Phishing-Seiten gelockt und betrogen werden oder auch die zuletzt erfolgte Umtauschaktion von Kreditkartendaten; Meldungen dieser Art erschüttern die Öffentlichkeit und führen zu einer steigenden Unsicherheit unter den Menschen, ob ihr Geld und ihre Daten denn tatsächlich vor Betrug und Missbrauch geschützt sind. Je mehr das Internet an Bedeutung gewinnt und der Mensch von IT-Systemen abhängig wird, desto höher liegt das Gefahrenpotenzial.

Die Praxis zeigt, dass trotz großer Sorgfalt und bestem Qualitätsmanagement auf Seiten der Betreiber Systeme kompromittiert und Daten ausgespäht werden. Ursachen hierfür sind oft Lücken und Fehler bei Administration und Softwareentwicklung, die bei der Konzeption oft nicht bedacht werden und bei denen die üblichen Kontrollmechanismen nicht greifen.

Aus diesen Gründen verfolgt ein Penetrationstest einen anderen Ansatz: Die Systeme des beauftragenden Kundenunternehmens werden unter Anwendung von Spezialwerkzeugen und -wissen aus der Perspektive eines Angreifers untersucht und attackiert. Hierbei wird genau das Angriffsszenario herbeigeführt, das ein realer Angreifer ebenfalls entdecken und ausnutzen würde. Aus dieser Sicht werden exakt die Probleme und Sicherheitsschwachstellen ans Licht gebracht, die Angriffe begünstigen. Somit kann dem Kunden ganz gezielt geholfen werden, vorhandene Mängel zu erkennen und diese zu beheben. Auf diese Weise unterstützen Penetrationstests den Kunden dabei, seine eigene IT-Landschaft nachhaltig zu stärken und im Endeffekt sicher zu betreiben.

Im Gegensatz zu anderen Prüf- und Qualitätssicherungsmethoden ist der Penetrationstest schnell und preiswert durchführbar und schafft harte, zweifelsfreie Fakten. Die Tatsache, dass im Rahmen von Penetrationstests die Mehrheit der Systeme kompromittiert wird, beweist ihre Daseinsberechtigung. Denn dies beweist, dass Systeme angreifbar und Sicherheitsschwächen vorhanden sind und dass konkreter Handlungsbedarf besteht. Um Penetrationstests jedoch wirksam durchführen zu können, müssen auch die rechtlichen Rahmenbedingungen beachtet werden.

Vertragsgestaltung von Firma und Penetrationstester

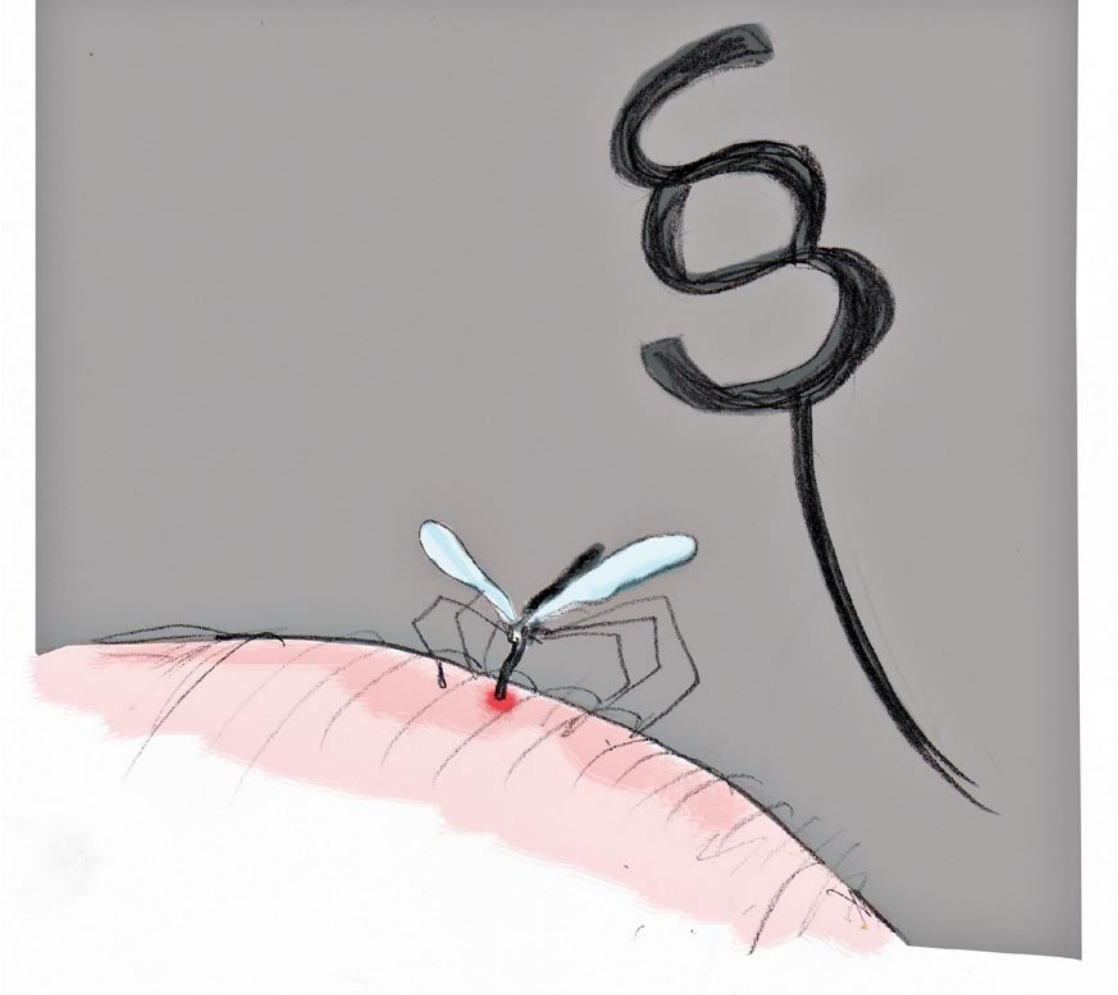
Die meisten Firmen vergeben Penetrationstests an externe Unternehmen. Dies ist in aller Regel auch sinnvoll, denn zum einen wäre das Unterhalten eines eigenen Penetrationstest-Teams teurer als die Beauftragung eines externen Dienstleisters und zum anderen würde ein eigenes Team weder unabhängig testen können noch in demselben Maße über eine Bandbreite unterschiedlichster Erfahrungen aus Prüfungen fremder IT-Umgebungen verfügen wie ein Unternehmen, das ausschließlich Penetrationstests anbietet.

> *» Das deutsche Strafrecht stellt unter gewissen Umständen sowohl den Besitz als auch den Einsatz von sogenannten Hackertools unter Strafe. «*

Um eine fruchtbare Zusammenarbeit zwischen dem beauftragenden Unternehmen und dem Penetrationstester sicherzustellen, sollte das Unternehmen den externen Dienstleister auf die Einhaltung absoluter Vertraulichkeit verpflichten. Zudem sind Haftungsfragen im Vorfeld zu klären. Aufgrund der heiklen Situation wird geraten, ein Sub-Contracting auszuschließen. Ein Penetrationstest ist eine Maßnahme der Qualitätssicherung – und muss auch selbst qualitätsgesichert werden. Eine Möglichkeit für Unternehmen den Penetrationstest im Gegenzug qualitätszusichern, ist, dem Test wenigstens in Teilen beizuwohnen und sich selbst von der Arbeit des Penetrationstesters zu überzeugen.

Der sogenannte Hackerparagraf: § 202 StGB

Das deutsche Strafrecht stellt unter gewissen Umständen sowohl den Besitz als auch den Einsatz von sogenannten Hacker-



Tools unter Strafe. Die Strafbarkeit hängt von der subjektiven Vorstellung des Handelnden ab – dies bedeutet, dass Behörden und Richter große Spielräume bei ihrer Entscheidungsfindung haben.

Um sich hier im Rahmen der Legalität zu bewegen, hat Rechtsanwalt Franz-Josef Schillo im Februar 2008 einen Artikel über die Probleme mit dem Hackerparagrafen verfasst, in dem er „7 goldene Regeln" für den rechtssicheren Umgang mit Hacker-Tools definiert:

1. Sammlung und Dokumentation von Hacker-Tools
2. Regelung zur Dokumentation und zum Einsatzzweck
3. Separierung und Zusatzsicherung der Hacker-Tools
4. Einschränkung und Staffelung der Zugriffsbefugnisse
5. Dokumentation der Zugriffe und Einsätze
6. Reguläre und Stichprobenkontrollen
7. Kontrolle der Kontrolleure und Dokumentation

Daher muss also der Penetrationstester mit erheblichem Aufwand sicherstellen, dass nicht der Hauch eines Verdachts des illegalen Handelns entstehen kann.

Da externe Penetrationstester sich mit den aufgeführten Schwierigkeiten beim Umgang mit Hacker-Tools regelmäßig beschäftigen und auseinandersetzen, sind sie Spezialisten auf diesem Gebiet. Durch eine Vergabe der Prüftätigkeit an sie können Unternehmen daher die Gefahr von rechtlichen Risiken minimieren. Auch Rechtsanwalt Dr. Jyn Schultze-Melling empfiehlt in einem Artikel im Handelsblatt vom 15. September 2007, dass Unternehmen aus diesen Gründen Penetrationstests durch eine Drittfirma durchführen lassen sollten.

Eine Berufsethik als Verhaltensgrundlage für Penetrationstester

Um also sich innerhalb der gegebenen Gesetzesgrenzen zu bewegen, ist es hilfreich, sein Verhalten auf einer ethischen Grundlage aufzubauen. Eine solche Grundlage bietet der vom Autor selbst verfasste Entwurf einer Berufsethik für Penetrationstester. Die darin formulierten Leitsätze können den Penetrationstester ganz konkret dabei unterstützen, eine ethische Grundlage für sein Handeln zu legen und oftmals unbewusste Gefahren zu umschiffen. Diese Leitsätze umfassen folgende Punkte:

- **Unabhängigkeit:** Penetrationstests durchführende Firmen testen nur in solchen Unternehmen, in denen sie weder bei der Konzipierung der IT-Umgebung noch der Einrichtung von Sicherheitsmaßnahmen beteiligt gewesen sind und an die sie auch keine eigene Software verkauft haben oder verkaufen wollen. Nur so kann sichergestellt werden, dass die Ergebnisse des Tests objektiv sind.
- **Vertraulichkeit:** Sowohl Identität der beauftragenden Firma als auch jegliche Einblicke in interne Netzwerke, Strukturen sowie in jegliche Daten, ebenso auch die, die dem Penetrationstester zur Verfügung gestellt werden, sind absolut vertraulich zu behandeln.
- **Provisionsverbot:** Die Annahme von Provisionen oder vergleichbaren Vorteilen ist untersagt.
- **Vorsicht:** Der Kunde ist über mögliche Risiken in Kenntnis zu setzen, die bei den Prüfungen entstehen können.
- **Professionalität und Qualitätsmanagement:** Die Arbeit hat professionell zu erfolgen und ist einem Qualitätsmanagement zu

unterziehen. Dabei leistet der Penetrationstester seine Arbeit nach bestem handwerklichem Wissen und ethischen Gewissen.

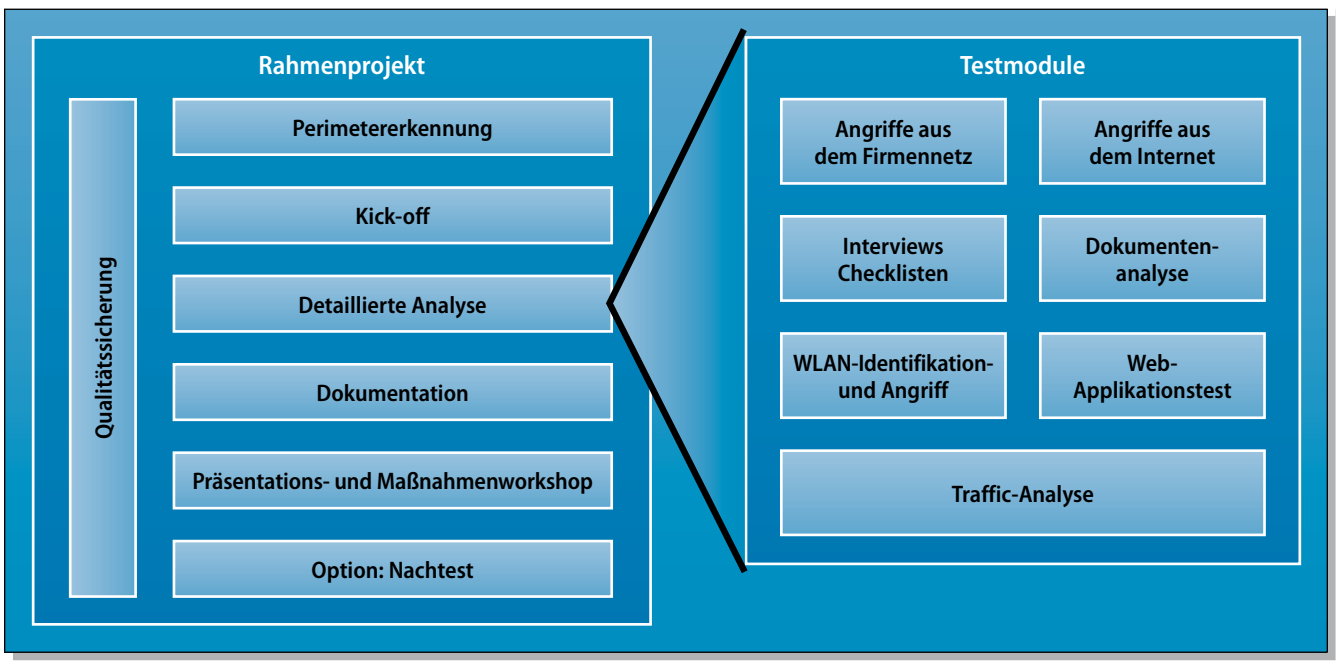
- **Verbindlichkeit:** Vertraglich zugesicherte und in Beratungsgesprächen mündlich getroffene Zusagen sind von den Mitarbeitern der Penetrationstests durchführenden Firma verbindlich einzuhalten.
- **Objektivität, Neutralität und Transparenz:** Schlussfolgerungen müssen objektiv sein und sind nachvollziehbar darzustellen.
- **Interessenskonflikte:** Interessenskonflikte zwischen Penetrationstestern und Kunden sind zu vermeiden und gegebenenfalls anzuzeigen und auszuräumen.
- **Striktes Legalitätsprinzip:** Die Gesetze der von Penetrationstests betroffenen Länder sind strikt einzuhalten, auch wenn Teilergebnisse eines Penetrationstests selbst einen Interessenskonflikt mit der vorgefundenen Gesetzgebung darstellen könnten. So kann die Aufdeckung von Schwachstellen in bestimmten Fällen Verstöße gegen bestehendes Recht begünstigen. Penetrationstester sind daher verpflichtet, sich mit der jeweiligen Gesetzeslage vertraut zu machen und sorgfältig darauf zu achten, dass ihre Arbeit innerhalb der vorgegebenen Gesetzesgrenzen abläuft.
- **Respekt vor Menschen:** Social-Engineering-Attacken sind Angriffe gegen das Verhalten von Menschen – diese werden, sofern sie überhaupt durchgeführt werden – ausschließlich nach vorheriger Ankündigung durchgeführt.
- **Korrektes Zitieren:** Wird fremdes Wissen bei der Arbeit herangezogen und verwertet, so sind die Quellen/Urheber korrekt auszuweisen.

Sorgfalt während des Penetrationstests

Penetrationstests gehen immer mit einem unvermeidbaren Risiko einher. Um die immanenten Risiken kalkulieren und möglichst auch beherrschen zu können, existieren eine Reihe von Maßnahmen, die für die gebotene Sorgfalt in der Umsetzung von Penetrationstests sorgen sollen:

1. Korrekte Aufklärung über Risiken vor Auftragsvergabe; gute Betreuung des Kunden im laufenden Projekt.
2. Durchführung eines Kick-off-Workshops anhand einer erprobten Checkliste unter Erstellung eines schriftlichen Protokolls.
3. Absolute Sorgfalt und Professionalität.
4. Durchführen von Penetrationstests erst nach schriftlichem Auftrag.
5. Prüfung der vom Kunden gelieferten Daten auf Korrektheit (z. B. IP-Ranges).
6. Durchführung des Tests durch ausgebildete und erfahrene Spezialisten.
7. Minimierung des Risikos durch Gestaltung des Prüfprojekts:
   - Langsame Scans (Reduktion der Bandbreite bzw. Request-Rate),
   - separates Testen einzelner Server,
   - Tests außerhalb der Geschäftszeit (z. B. nachts/am Wochenende),
   - prüfen von Testsystemen,
   - Fähigkeit, den Test „auf Zuruf“ abzubrechen,
   - Wahl nicht-invasiver Prüfmethoden,

Abb. 1 *Testaufbau*



- Gewährleistung, dass ein abgestürztes System wieder gestartet wird.

Eine Beschränkung auf die Testmethoden, mit denen keinerlei Risiko einhergeht, ist nicht zu empfehlen – die Aussagekraft der Prüfung wäre gering.

Abbildung 1 verdeutlicht, wie ein sinnvoller Aufbau von Penetrationstests aussehen und welche Testmodule ein solcher Test umfassen kann.

» Eine Beschränkung auf die Testmethoden, mit denen keinerlei Risiko einhergeht, ist nicht zu empfehlen. Die Aussagekraft wäre gering. «

Prüfungen von Systemen Dritter

Wenn Unternehmen ihren IT-Betrieb ganz oder teilweise an Dienstleister vergeben, können sie nicht eigenmächtig einen Penetrationstest beauftragen, sondern müssen vom Dienstleister eine Einwilligung zur Durchführung eines solchen geben. Ohne diese stellt ein Penetrationstest eine Straftat nach § 202 StGB dar – daher ist es wichtig, zuvor eine schriftliche Freigabe des oder der Eigentümer einzuholen. Als solche kommen infrage:

1. der Eigentümer der Hardware
2. der Eigentümer der Domain
3. der (Haupt-)Nutzer des Systems
4. der Eigentümer der IP-Adresse
5. der Inhaber der Verfügungsgewalt des Systems

Ist ein Unternehmen von einem Lieferanten in hohem Maße abhängig, so sind Lieferantenaudits allgemein üblich und sinnvoll. Lagert man vertrauliche Daten bei Lieferanten (Auftragsdatenverarbeitung), so sollten die Lieferantenaudits auch Penetrationstests umfassen.

Um hier keine Schwierigkeiten zu bekommen, empfiehlt es sich, bereits in Outsourcing-Verträgen ein Prüfrecht zu verankern.

Datenschutzgesetz, Bankgeheimnis etc.

Es ist durchaus möglich oder sogar wahrscheinlich, dass der Penetrationstester im Rahmen der Prüfung auf Kundendaten, personenbezogene Informationen oder auf andere vertrauliche Daten stößt. Je nach Branche ist der Penetrationstester auf die besondere Sorgfaltspflicht beim Umgang mit diesen Daten zu verpflichten.

Reverse Code Engineering

Im Rahmen von Penetrationstests werden oft Systeme geprüft, zu deren Software der Quelltext nicht verfügbar ist und daher nicht analysiert werden kann, dies betrifft beispielsweise Flash-Plug-ins, ein PDF-Viewer oder ein proprietärer Webserver. Soll beispielsweise geprüft werden, ob eine Standard-Software mit einer Hintertüre (Backdoor) versehen ist, so kann technisch gesehen eine sogenannte Dekompilierung durchgeführt werden, obwohl unter Juristen umstritten ist, ob diese Prüfmethode gemäß § 69 e UrHg rechtlich unbedenklich oder problematisch ist. Debugging sowie Disassemblieren sind in Deutschland legal. Daher muss bei Reverse Code Engineering stets geprüft werden, welche Prüfmethoden erlaubt sind.

Rechtspflicht Penetrationstest?

Eine explizite Rechtspflicht zur Durchführung von Penetrationstests besteht nicht, lässt sich aber aus einer Vielzahl von Gesetzen und Regelungen ableiten. So fordert das KontrAG, dass bedeutsame Unternehmensrisiken zu identifizieren und zu überwachen sind. Basel II macht die IT-Security kreditrelevant. Beim Abschluss von Versicherungen hat also ein professionelles Security-Management Einfluss auf die Versicherungsprämie; bei der Aufnahme von Krediten hat es Einfluss auf den zu entrichtenden Zins. Den Schutz personenbezogener Daten fordert das BDSG – und die Leitlinien der „Grundsätze ordnungsmäßiger Buchführung“ (GoB, GoBS) erzwingen verlässliche IT-Systeme. In manchen Branchen gelten zusätzliche Regelungen (Kreditwesengesetz, Verordnungen der BAFin (Bundesanstalt für Finanzdienstleistungsaufsicht), Staatsvertrag für Mediendienste, Datenschutzgesetz für Teledienste, Telekommunikationsgesetz etc.), die ebenso auf einer starken IT-Sicherheit fußen. Eine sichere IT-Umgebung erreichen Firmen jedoch nur, wenn sie Penetrationstests durchführen lassen und regelmäßig ihre IT-Systeme auf Sicherheitsschwächen prüfen lassen.

Links und Literatur

Bundesamt für Sicherheit in der Informationstechnik: Durchführungskonzept für Penetrationstests, 2003, http://www.bsi.bund.de/literat/studien/pentest/penetrationstest.pdf, Abruf am 25.2.2004.

Schillo, Franz-Josef: Probleme mit dem Hackerparagraphen, Network Computing, 26.02.2008.

Schmundt, Hilmar: Bezahlter Einbruch, DER SPIEGEL 9. Mai 2005.

Schreiber, Sebastian: Entwurf einer Berufsethik für Penetrationstester, DuD, 4/2009 [Schultze-Melling 2007] Schultze-Melling, Jyn: Manager in der Zwickmühle, Handelsblatt, 18.09.2007.

Autor

Sebastian Schreiber
ist Diplom-Informatiker und seit 1998 Geschäftsführer der SySS GmbH und erfolgreich im Bereich IT-Sicherheit tätig. Ferner ist er Experte für Penetrationstests und im In- und Ausland bekannt für seine Live-Hacking-Demonstrationen.